ESE Hospital
San Juan de Dios
Santa Fe de Antioquia

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

CLAUDIA MARIA CALDERON RUEDA
GERENTE

JUAN DAVID ECHEVERRY
INGENIERO DE SISTEMAS

2023

Contenido

1. INTRODUCCIÓN

Este documento busca lograr la implementación en el Hospital San Juan de Dios las mejoras prácticas dadas por el Departamento de Administrativo de la Función Pública con su estrategia MIPG y el Ministerio de las Tecnologías e Información en el diagnóstico, planificación, implementación, gestión y mejoramiento continuo, del Modelo de Seguridad yPrivacidad de la Información.

El Modelo de Seguridad y Privacidad de la Información, pretende lograr en la institución y sus clientes internos, externos y partes interesadas confianza en el manejo de la información garantizando para cada uno la privacidad, continuidad, integralidad y disponibilidad de los datos.

2. OBJETIVOS

OBJETIVO GENERALES

Generar un documento institucional guiado en lineamientos de buenas prácticas en seguridad y Privacidad de la información.

OBJETIVO ESPECIFICO

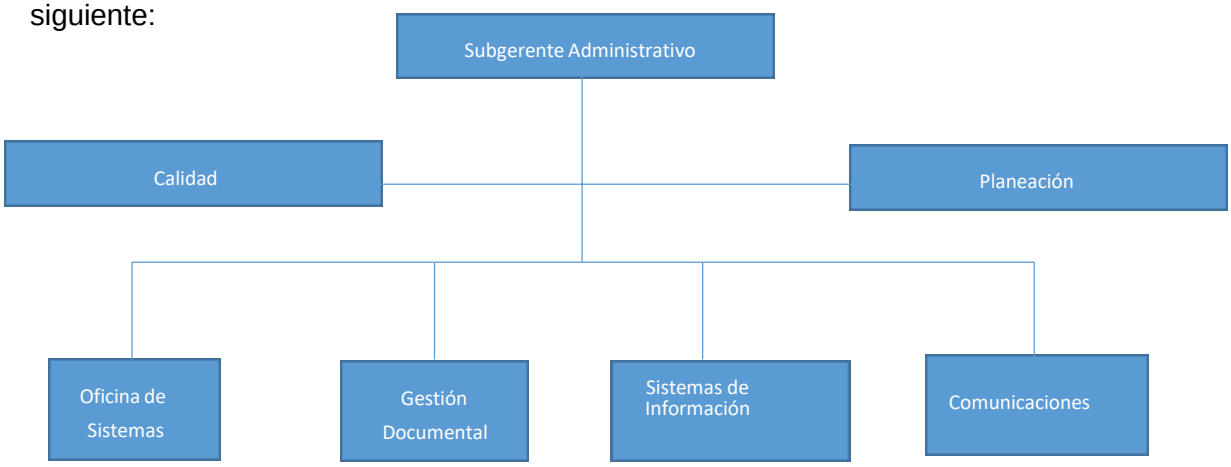
- Promover el uso de mejores prácticas de seguridad de la información en la institución
- Establecer los mecanismos de aseguramiento físico y digital, para fortalecer la confidencialidad, integridad, disponibilidad, autenticidad, y privacidad de la información de la ESE Hospital San Juan de Dios de Santa Fe de Antioquia.
- Asegurar y hacer uso eficiente y seguro de los recursos de Tecnologías de Información y Comunicaciones, así como aquellos equipos biomédicos que almacena información referente a los servicios prestados, con el fin de garantizar la continuidad de la prestación de los servicios.
- Dar cumplimiento a los requisitos legales y normativos en materia de Seguridad y Privacidad de la Información, Seguridad Digital y protección de la información personal.
- Minimizar el riesgo de vulnerabilidad de la información en el desarrollo de los procesos.
- Optimizar la labor de acceso a la información pública

3. ALCANCE

Aplica a todos los niveles asistenciales y administrativos de la ESE Hospital San Juan de Dios de Santa Fe de Antioquia, sus funcionarios, contratistas, proveedores, usuarios, docentes, estudiantes que realicen prácticas, pasantías o trabajos de grado, bajo el marco de un contrato y/o convenio académico y cooperantes, adicionalmente todas aquellas personas o terceros que en razón del cumplimiento de sus funciones y las de la ESE compartan, utilicen, recolecten, procesen, intercambien o consulten su información, así como a los Entes de Control, que accedan ya sea interna, remotamente o vía internet a cualquier tipo de información, independientemente de su ubicación. Así mismo, esta lo dispuesto en este documento y su implementación aplica a toda la información creada, procesada o utilizada por la ESE Hospital San Juan de Dios, sin importar el medio, formato, presentación o lugar en el cual se encuentre.

4. RESPONSABLES

La estructura organizacional de los procesos responsables de la realización del plan es la siguiente:



- Subgerente Administrativo y Financiero
- Profesional Universitarios de Planeación
- Profesional Universitarios de Calidad
- Ingeniero de Sistemas
- Técnico en gestión documental
- Profesional Universitarios Gesis
- Comunicadora social

5. MARCO CONCEPTUAL (DEFINICIONES RELEVANTES)

- **Acceso a la Información Pública:** Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceder a la información pública en posesión o bajo control de sujetosobligados. (Ley 1712 de 2014, art 4)
- **Activo:** En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas…) que tenga valor para la organización. (ISO/IEC27000).
- **Activo de Información:** En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal.

- **Archivo:** Conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o entidad públicao privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, o como fuentes de la historia.También se puede entender como la institución que está al servicio de la gestión administrativa, la información, la investigación y la cultura. (Ley 594 de 2000, art 3)
- **Amenazas:** Causa potencial de un incidente no deseado, que puedeprovocar daños a un sistema o a la organización. (ISO/IEC 27000).
- **Análisis de Riesgo:** Proceso para comprender la naturaleza del riesgo ydeterminar el nivel de riesgo. (ISO/IEC 27000).
- **Auditoría:** Proceso sistemático, independiente y documentado para obtener evidencias de auditoria y obviamente para determinar el grado en el que se cumplen los criterios de auditoria. (ISO/IEC 27000).
- **Autorización:** Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales (Ley 1581 de 2012, art 3)
- **Bases de Datos Personales:** Conjunto organizado de datos personales quesea objeto de Tratamiento (Ley 1581 de 2012, art 3)
- **Ciberseguridad:** Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética. (CONPES 3701).
- **Ciberespacio:** Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizadopara la interacción entre usuarios. (Resolución CRC 2258 de 2009).
- **Control:** Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de lainformación por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.
- **Datos Abiertos:** Son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposiciónde cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos (Ley 1712 de 2014, art 6)
- **Datos Personales:** Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3).
- **Datos Personales Públicos:** Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad decomerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente

ejecutoriadas que no estén sometidas a reserva. (Decreto 1377 de 2013, art3)

- **Datos Personales Privados:** Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular. (Ley 1581 de 2012, art 3 literal h)
- **Datos Personales Mixtos:** Para efectos de esta guía es la información quecontiene datos personales públicos junto con datos privados o sensibles.
- **Datos Personales Sensibles:** Se entiende por datos sensibles aquellos queafectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos. (Decreto 1377 de 2013, art 3)
- **Declaración de aplicabilidad:** Documento que enumera los controles aplicados por el Sistema de Gestión de Seguridad de la Información – SGSI, de la organización tras el resultado de los procesos de evaluación y tratamiento de riesgos y su justificación, así como la justificación de las exclusiones de controles del anexo A de ISO 27001. (ISO/IEC 27000).
- **Derecho a la Intimidad:** Derecho fundamental cuyo núcleo esencial lo constituye la existencia y goce de una órbita reservada en cada persona, exenta de la intervención del poder del Estado o de las intromisiones arbitrarias de la sociedad, que le permite a dicho individuo el pleno desarrollo de su vida personal, espiritual y cultural (Jurisprudencia Corte Constitucional).
- **Encargado del Tratamiento de Datos:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del Responsable del Tratamiento. (Ley 1581 de 2012, art 3)
- **Gestión de incidentes de seguridad de la información:** Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000).
- **Información Pública Clasificada:** Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que setrate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6)
- **Información Pública Reservada:** Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada deacceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento dela totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6)
- **Ley de Habeas Data:** Se refiere a la Ley Estatutaria 1266 de 2008.

- **Ley de Transparencia y Acceso a la Información Pública:** Se refiere a laLey Estatutaria 1712 de 2014.
- **Mecanismos de protección de datos personales:** Lo constituyen las distintas alternativas con que cuentan las entidades destinatarias para ofrecerprotección a los datos personales de los titulares tales como acceso controlado, anonimización o cifrado.
- **Plan de continuidad del negocio:** Plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un eventoimprevisto que las ponga en peligro. (ISO/IEC 27000).
- **Plan de tratamiento de riesgos**: Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantarlos controles necesarios para proteger la misma. (ISO/IEC 27000).
- **Privacidad:** En el contexto de este documento, por privacidad se entiende elderecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones que a ella le compete realizar y que generan en las entidades destinatarias del Manual de GEL la correlativa obligación de proteger dicha información en observancia del marco legal vigente.
- **Registro Nacional de Bases de Datos:** Directorio público de las bases de datos sujetas a Tratamiento que operan en el país. (Ley 1581 de 2012, art 25)
- **Responsabilidad Demostrada:** Conducta desplegada por los Responsables o Encargados del tratamiento de datos personales bajo la cual a petición de la Superintendencia de Industria y Comercio deben estar en capacidad de demostrarle a dicho organismo de control que han implementado medidas apropiadas y efectivas para cumplir lo establecido en la Ley 1581 de 2012 y sus normas reglamentarias.
- **Responsable del Tratamiento de Datos:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos. (Ley 1581 de 2012, art 3).
- **Riesgo:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).
- **Seguridad de la información:** Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).
- **Sistema de Gestión de Seguridad de la Información SGSI:** Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos,procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000).
- **Titulares de la información:** Personas naturales cuyos datos personales sean objeto de Tratamiento. (Ley 1581 de 2012, art 3)

- **Tratamiento de Datos Personales:** Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión. (Ley 1581 de 2012, art 3).
- **Trazabilidad:** Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad. (ISO/IEC 27000).
- **Vulnerabilidad:** Debilidad de un activo o control que puede ser explotada poruna o más amenazas. (ISO/IEC 27000).
- **Partes interesadas (Stakeholder):** Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.

6. MARCO NORMATIVO

- Anexo 1 - Resolución 3564 de 2015 - Reglamenta aspectos relacionados con laLey de Transparencia y Acceso a la Información Pública
- Decreto Reglamentario Único 1081 de 2015 - Reglamento sobre la gestión de la información pública
- Título 9 - Decreto 1078 de 2015 - Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones
- Ley 1712 de 2014 - Ley de Transparencia y acceso a la información pública
- Ley 57 de 1985 -Publicidad de los actos y documentos oficiales
- Ley 594 de 2000 - Ley General de Archivos
- Título 9 - Decreto 1078 de 2015 - Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones
- Título 9 - Decreto 1078 de 2015 - Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones
- Ley Estatutaria 1757 de 2015 - Promoción y protección del derecho a laparticipación democrática
- Título 9 - Decreto 1078 de 2015 - Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones
- Ley estatutaria 1618 de 2013: Ejercicio pleno de las personas con discapacidad

- Título 9 - Decreto 1078 de 2015 - Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones
- Ley 1437 de 2011: Código de Procedimiento Administrativo y de lo Contencioso Administrativo
- Acuerdo 03 de 2015 del Archivo General de la Nación Lineamientos generalessobre la gestión de documentos electrónicos
- Título 9 - Decreto 1078 de 2015 - Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones
- Acuerdo 03 de 2015 del Archivo General de la Nación Lineamientos generalessobre la gestión de documentos electrónicos
- Decreto 019 de 2012 - Suprimir o reformar regulaciones, procedimientos ytrámites innecesarios existentes en la Administración Pública
- Decreto 2364 de 2012 - Firma electrónica
- Ley 962 de 2005 - Racionalización de trámites y procedimientos administrativos procedimientos administrativos
- Decreto 1747 de 2000 - Entidades de certificación, los certificados y las firmas digitales
- Ley 527 de 1999 - Ley de Comercio Electrónico
- Decreto Ley 2150 de 1995 - Suprimen y reforman regulaciones, procedimientoso trámites innecesarios existentes en la Administración Pública
- Título 9 - Decreto 1078 de 2015 - Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones
- Ley Estatutaria 1581 de 2012 - Protección de datos personales
- Ley 1266 de 2008 - Disposiciones generales de habeas data y se regula elmanejo de la información

7. DESCRIPCIÓN DEL PLAN

POLITICA DE SEGURIDAD Y CONFIDENCIALIDAD DE LA INFORMACION

El equipo de colaboradores y el Gerente del Hospital San Juan de Dios se comprometen a garantizar la confidencialidad, seguridad e integralidad de la información de los usuarios y su familia, clientes internos y externos en cuanto a seguridad lógica y física de los activos

de la información, fomento de canales de comunicación que garanticen acceso y transparencia de la información pública a través de uso adecuado de las TICS, cumpliendocon las disposiciones generales para la protección de datos, aportando al cumplimiento de la Misión, Visión y objetivos estratégicos de la institución.

El siguiente plan está diseñado para cumplir la fase de determinar el estado actual de la gestión de seguridad y privacidad de la información al interior de la Entidad. Para realizar este paso los responsables del plan deben efectuar la recolección de la información con la ayuda de la guía de autoevaluación, guía de encuesta y guía metodológica de las pruebas de efectividad del Modelo de Seguridad y Privacidad de la Información (**MSPI**)

OBJETIVOS DE LA POLITICA DE GESTION DE CALIDAD

- Garantizar la protección de datos personales de usuarios, clientes, proveedores y trabajadores tanto en los medios físicos como electrónicos.

- Controlar el uso efectivo de equipos de cómputo que garantice la confidencialidad, seguridad e integralidad de la información de los usuarios incluyendo.

- Fortalecer el conocimiento y la adherencia en el plan de contingencia en caso decaída del sistema de información

ALCANCE:

Esta política abarca los siguientes procesos:

ESTRATEGICO: TODOS LOS PROCESOS

MISIONAL: TODOS LOS PROCESOS

DE APOYO: TODOS LOS PROCESOS

7.1 SEGURIDAD DE LA INFORMACIÓN EN EL TALENTO HUMANO

Todos los funcionarios de la ESE Hospital San Juan de Dios de Santa Fe de Antioquia, independiente del tipo de vinculación laboral o contractual, o de los procesos al que pertenezca y del nivel de funciones o actividades que desempeñe deben contar con un perfil de uso de los recursos de información, (no se incluye el personal de servicios generales). La responsabilidad de custodia de cualquier documento o archivo generado dentro de la entidad, usado o producido por algún funcionario y/o contratista que se retira, recae en los subdirectores Científico y Administrativo para el personal de planta y en el supervisor del contrato para el resto de personal, la oficina de las TICS es la encargada de la realización de las copias de seguridad para el caso de información electrónica que repose en los computadores; aclarando que el proceso de cadena de custodia de la información debe hacer parte integral de un procedimiento de terminación de la relación contractual o de cambio de cargo.

7.2 SEGURIDAD FÍSICA Y DEL ENTORNO

Los servidores que contengan información institucional deben estar ubicados en el DataCenter que cuenta en el Hospital: protegidos con controles de acceso y seguridad física, sistemas eléctricos regulados, respaldados por fuentes de potencia ininterrumpida (UPS) y con circuitos alternos de entrada de corriente; además con monitoreo permanente de sensores de humo y temperatura.

7.3 REPORTE Y REVISIÓN DE INCIDENTES DE SEGURIDAD

El personal vinculado a la ESE Hospital San Juan de Dios y que tenga acceso al sistema de información SERVINTE CLINICAL SUITE, debe realizar el reporte de todas las presuntas violaciones de seguridad detectadas, mediante un correo electrónico o en la plataforma web http://soporte.hospitalantioquia.com/, dirigido a la Coordinación TICS. En el caso de no tener acceso al sistema de información se debe realizar el reporte inmediato al supervisor del proceso, quién lo realizará a su respectivo supervisor del contrato.

7.4 PROTECCIÓN CONTRA MALWARE Y HACKING

Todos los equipos de informática de la ESE deben estar protegidos de amenazas de malware, instalación de software no autorizado y hackeo mediante un conjunto de acciones que se describen a continuación y cuyo objetivo es el de disminuir la probabilidad de un evento que genere daños en la plataforma informática.

a. En cada equipo se configurarán dos tipos de cuentas para el sistema operativo: la cuenta de perfil administrador es de exclusivo manejo de la oficina TICS, la cuenta de usuario normal es para el ingreso de los funcionarios que usan el equipo.

b. Cada equipo contará con software antivirus, el cual será actualizado en cada mantenimiento preventivo que se realiza al mismo, buscando un máximo de 6 meses para cada actualización.
c. Instalación de un software tipo congelador en los equipos buscando restaurar su estado original simplemente con un reinicio.

7.5 COPIAS DE SEGURIDAD

Es responsabilidad de todo funcionario realizar la copia de seguridad de la información manejada en cada equipo asignado, para este proceso se encuentra disponible una carpeta de copias que a su vez el agente realiza el backups cada cierto periodo dependiendo de la importancia de la información. Estas copias reposaran en un servidor destinado para este propósito. Este proceso será sujeto de auditoría por parte de la oficina TICS, quien informará a las respectivas subdirecciones sobre el incumplimiento en estas actividades. Las copias de seguridad de las bases de datos y documentos almacenados en los servidores ubicados en el datacenter de la institución, son realizadas por la oficina TICS, de acuerdo al procedimiento ya definido.

7.6 INTERCAMBIO DE INFORMACIÓN CON ENTIDADES EXTERNAS

Las peticiones o solicitudes de información por parte de entes externos deben ser aprobadas por la Gerencia previamente, quién determinará las personas responsables del manejo y custodia de dicha información. Todo requerimiento debe haber sido previamente radicado en la oficina de gestión documental, cumpliendo los procedimientos institucionales establecidos para la gestión documental. La información entregada será de acuerdo a la clasificación de confidencialidad establecida en el inventario de activos de información.

7.7 SERVICIO DE COMUNICACIÓN DE DATOS INTERNET

Este servicio será administrado por la oficina TICS, el acceso de los usuarios a internet estará limitado solo para aquellos procesos en donde es requerido y mediante el uso de diferentes perfiles, los cuáles restringirán el horario, páginas visitadas y posibilidad de descarga de información, buscando mitigar el riesgo de un ataque web. Se debe garantizar una conexión mínima para los procesos vitales, por lo tanto, se debe contar con dos proveedores diferentes que permitan realizar un respaldo de cada uno por fallo.

a. El acceso a internet está restringido solamente a funcionarios de la institución que en el normal desarrollo de sus procesos lo requieran, y será administrado por medio de un servidor proxy y filtros de control de navegación. El número de usuarios por área será determinado de acuerdo a la capacidad del servicio contratado por la empresa con su proveedor externo de conectividad.

b. No se permite la descarga de videos o música, el acceso a sitios cuyo contenido involucre compras, pornografía, canales de televisión o radio en línea, actos delictivos y aquellos considerados por TICS, como potencialmente dañinos para la seguridad informática de la

ESE.

c. Como página de inicio de los navegadores debe ser establecida la página web institucional www.esehospitalsantafedeantioquia.gov.co.

d. Los servicios de correo no pueden ser utilizados como soporte al desarrollo de actividades ilegales, ni pueden ser utilizados como herramientas de publicidad institucional sin la debida autorización de la gerencia.

e. En el caso de utilización de los servicios de correo para el intercambio de información con otras empresas, se debe colocar el nombre completo del funcionario y su cargo en los datos del remitente.

f. El proceso TICS debe generar registros de la navegación y los accesos de los usuarios a Internet, así como establecer e implantar el monitoreo sobre la utilización del servicio de Internet.

Para la red de datos institucional se debe contar con un Sistema de Detección de intrusos que permita estarla monitoreando permanentemente, de igual manera un firewall de altas prestaciones para la protección contra amenazas externas.

7.8 COMUNICACIONES INTERNAS Y EXTERNAS

Todo lo referente a la generación de comunicaciones tanto internas como externas, estará regida por "Política de Comunicaciones de la ESE Hospital San Juan de Dios de Santa Fe de Antioquia''

8. ANALISIS Y PRIORIZACION DE INICIATIVAS

La E.S.E Hospital San Juan de Dios de Santa Fe de Antioquia ha identificado las siguientes iniciativas buscando garantizar el avance de la institución en la construcción de una arquitectura de seguridad de la información.

No.	Descripción	Estrategia de Seguridad de la información			
		Modelo de seguridad de la información	**Gestión de riesgos de seguridad**	**Desarrollo y gestión del programa de seguridad de la información**	**Gestión de incidentes de seguridad de la información**
1	Documentar, Implementar, evaluar y mejorar el Plan de Seguridad y Privacidad de la información	X			

2	Definir e integrar la seguridad de la información en los procesos institucionales buscando asegurar que los riesgos de seguridad de la información se identifiquen y traten como parte del proceso	X			
3	Diseñar, documentar, implementar, evaluar y mejorar un programa anual de capacitaciones y sensibilización sobre seguridad de la información dirigido a los colaboradores, empleados, terceros y partes interesadas	X			
4	Documentar y normalizar el Plan de Tratamiento de Riesgos de seguridad de la información		X		
5	Actualizar los activos de información y realizar su valoración por criticidad para la entidad e identificar los riesgos de seguridad de la información asociados		X		
6	Diseñar los planes de continuidad del negocio que contemplen los procesos críticos para la entidad		X		
7	Documentar, Implementar y realizar pruebas de los planes de continuidad de negocio, así mismo Aprobar los planes de continuidad por La alta dirección.		X		
8	Implementar arquitecturas redundantes en dispositivos de seguridad Firewall y Dispositivos de comunicaciones Core			X	

9	Definir y establecer un procedimiento formal para el tratamiento de información de producción en ambientes de desarrollo y prueba, en el cual se establezcan controles para proteger la Confidencialidad de la información.			X	

No.	**Descripción**	Estrategia de Seguridad de la información			
		Modelo de seguridad de la información	**Gestión de riesgos de seguridad**	**Desarrollo y gestión del programa de seguridad de la información**	**Gestión de incidentes de seguridad de la información**
10	Definir y establecer las políticas y procedimientos relacionados con la gestión de usuarios privilegiados que administren las plataformas tecnológicas (servidores, elementos de red, bases de datos), así como a las funciones de negocio que Requieren el uso deprivilegios.			X	
11	Monitorear el cumplimientodel ciclo de vida de gestión de usuarios (creación, modificación, activación, desactivación, eliminación, entre otros) verificando quese cumple para todas las Aplicaciones.			X	

No.	Descripción	Estrategia de Seguridad de la información			
		Modelo de seguridad de la información	Gestión de riesgos de seguridad	Desarrollo y gestión del programa de seguridad de la información	Gestión de incidentes de seguridad de la información
12	Implementar una solución como servicio de Firewall de aplicaciones Web para la protección de aplicaciones Web			X	
13	Operar y mantener el sistema de gestión de seguridad de la Información SGSI, incluyendo todos los procesos de la entidad.			X	
14	Implementar y monitorear los indicadores del sistema de gestión de seguridad de la información	X			

9. DEFINICION DEL PORTAFOLIO DE PROCESOS

En esta etapa, después del análisis y priorización de iniciativas, se define el portafolio de proyectos del plan deseguridad y privacidad de la información, agrupados en proyectos relacionados con:

1. Gobierno o modelo de seguridad de información.
2. Gestión de riesgos de Seguridad.
3. Desarrollo y gestión del plan de seguridad de la información.
4. Gestión de incidentes de seguridad de la información.

	Iniciativa	Proyectos		
		Descripción	Avances	Requiere recursos financieros
1	Documentar, Implementar, evaluar y mejorar el Plan de seguridad y Privacidad de la Información.	Implementar, evaluar y mejorar el Plan de Seguridad y Privacidad de la Información	En proceso	SI

2	Definir e integrar la seguridad de la informaciónen los procesos institucionales buscando asegurar que los riesgos de seguridad de la informaciónse identifiquen y traten como parte del proceso	Integrar la seguridad de la información en los procesos institucionales	No iniciado	No
3	Diseñar, documentar, implementar, evaluar y mejorar un programa anual de capacitaciones y sensibilización sobre seguridad de la información dirigido a los colaboradores, empleados, terceros y partes interesadas	Diseñar ,documentar, implementar y evaluar el programa anual de capacitaciones y sensibilización sobre seguridad de la información dirigido a los colaboradores, empleados, terceros y partes interesadas	No iniciado	Si
4	Actualizar los activos de información y realizar su valoración por criticidad para la entidad e identificar los riesgos de seguridad de la información asociados	Actualizar la matriz de activos de información y publicaciones por criticidad para la entidad eidentificar los riesgos de seguridad de la información asociados	En proceso	No
5	Gestionar el Tratamiento de riesgos de seguridad de la información de los riesgos Identificados en cada uno de los procesos.	Gestionar el Tratamiento de riesgos de seguridad de la información de los riesgos Identificados en cada uno delos procesos.	No iniciado	No
6	Diseñar los planes de continuidad del negocio que contemplen los procesos críticos para la entidad	Diseñar los planes de continuidad del negocio quecontemplen los procesos críticos para la entidad	No iniciado	No
7	Documentar, Implementar y realizar pruebas de los planes de continuidad de negocio, así mismo Aprobarlos planes de continuidad Por la alta dirección.	Documentar, Implementar y realizar pruebas de los planes de continuidad de negocio, asímismo Aprobar los planes de continuidad por la alta Dirección.	No iniciado	No
8	Implementar arquitecturas redundantes en dispositivos de seguridad Firewall y Dispositivos de comunicaciones Core	Gestionar la adquisición de herramientas para soportar la infraestructura del Datacenter,en esquemas de alta disponibilidad para dispositivos de seguridad Firewall y Dispositivos de comunicaciones Core.	En proceso	Si

9	Definir y establecer un procedimiento formal para el tratamiento de información de producción en ambientes de desarrollo y prueba, en el cual se establezcan controlespara proteger la confidencialidad de la información.	Definir y establecer un procedimiento formal para el tratamiento de información de producción en ambientes de desarrollo y prueba, en el cual se establezcan controles para proteger la confidencialidad de la información.	No iniciado	No
10	Definir y establecer las políticas y procedimientos relacionados con la gestión de usuarios privilegiados queadministren las plataformas tecnológicas (servidores, elementos de red, bases de datos), así como a las funciones de negocio que requieren el uso de Privilegios.	Definir y establecer las políticas y procedimientos relacionados con la gestión de usuarios privilegiados que administren las plataformas tecnológicas (servidores, elementos de red, bases de datos), así como a las funciones de negocio que requieren el uso de privilegios.	No iniciado	No
11	Monitorear el cumplimiento del ciclo de vida de gestión de usuarios (creación, modificación, activación, desactivación, eliminación, entre otros) verificando que se cumple para todas las aplicaciones.	Definir y establecer las políticas y procedimientos relacionados con la gestión deusuarios privilegiados que administren las plataformas tecnológicas (servidores, elementos de red, bases de datos), así como a las funciones de negocio que Requieren el uso de privilegios.	No iniciado	No
12	Implementar una solución como servicio de Firewall de aplicaciones Web para la protección de aplicaciones Web	Implementar una solución como servicio de Firewall de aplicaciones Web para la protección de aplicaciones Web	En proceso	No
13	Operar y mantener el sistema de gestión de seguridad de la información SGSI, incluyendo todos los procesos de la entidad.	Operar y mantener el sistema de gestión de seguridad de la información SGSI, incluyendo Todos los procesos de la entidad.	No iniciado	No
14	Implementar y monitorear los indicadores del sistema de gestión de seguridad dela información	indicadores del sistema de gestión de seguridad de la información	No iniciado	No

10. PLAN DE ACCION

	Priorización de los Proyectos				
	Descripción	Prioridad Año 2021	Prioridad Año 2022	Prioridad Año 2023	Prioridad Año 2024
1	Implementar, evaluar y mejorar el Plan de Seguridad y Privacidad de la Información	X			
2	Integrar la seguridad de la información en los procesos institucionales		X		
3	Diseñar y documentar programa anual de capacitaciones y sensibilización sobre seguridad de la información dirigido a los colaboradores, empleados, terceros y partes interesadas			X	
	Implementar y evaluar el programa anual de capacitación y sensibilización sobre seguridad de la información dirigido a los colaboradores, empleados, terceros y partes interesadas			X	
4	Actualizar la matriz de activos de información y publicaciones por criticidad para la entidad e identificarlos riesgos de seguridad de la información asociados			X	
5	Documentar y normalizar el Plan de Tratamiento de riesgos de Seguridadde la información.			X	
6	Diseñar los planes de continuidad del negocio que contemplen los procesos			X	
7	Documentar, Implementar y realizar pruebas de los planes de continuidadde negocio, así mismo Aprobar los planes de continuidad por la alta dirección.			X	
	Gestionar la adquisición de herramientas para soportar la infraestructura del	X			

8	Datacenter, en esquemas de alta disponibilidad paradispositivos de seguridad Firewall y Dispositivos de comunicaciones Core.				
9	Definir y establecer las políticas y procedimientos relacionados con la gestión de usuarios privilegiados que administren las plataformas tecnológicas (servidores, elementos de red, bases de datos), así como a las funciones de negocio que requieren el uso de privilegios.			X	
10	Definir y establecer las políticas y procedimientos relacionados con la gestión de usuarios privilegiados que administren las plataformas tecnológicas (servidores, elementos dered, bases de datos), así como a las Funciones de negocio que requieren eluso de privilegios.			X	
11	Implementar una solución como servicio de Firewall de aplicacionesWeb para la protección de aplicaciones Web	X			
12	Implementar y monitorear los indicadores del sistema de gestión de seguridad de la información	X			

11. BIBLIOGRAFÍA

Ministerio de las TCI

http://www.mintic.gov.co/gestionti/615/w3-propertyvalue-7275.html

Ministerio de las TCI

https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf

Escuela Tecnológica

http://www.itc.edu.co/es/nosotros/seguridad-informacion

1. CONTROL DE CAMBIOS					
VERSIÓN	**FECHA**	**DESCRIPCIÓN**	**ELABORÓ**	**REVISÓ**	**APROBÓ**
01	Enero 2023	Elaboración del plan	Juan David Echeverry – Líder de sistemas	Nallybe Durán – Subgerente de Calidad	Claudia María Calderón – Gerente